IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 10/605,349   Confirmation No.: 2348
Applicant: : Peter L. Bergh
Filed: : September 24, 2003
Title: : System and Method for Presentation Integrity
TC/A.U. : 2132
Examiner: : Venkatanaray Perungavoor

Docket No. : 014607.000001
Customer No. : 62,616

Mail Stop: AF
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF IN COMPLIANCE WITH 37 CFR 41.37

In response to the Notice of Panel Decision from Pre-Appeal Brief Review as mailed December 17, 2007, this appeal brief is being submitted.

I. Real Party in Interest

The real party in interest is The Boeing Company, assignee of record.

II. Related Appeals and Interferences

There are no other appeals or interferences, known to the Appellants, or Appellants' legal representatives, which will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

III. Status of Claims

Claims 1-7, 9-51, 53-73, 75-90, 92-100, 103-114, 132, 134-141 are pending. Claims 8, 52, 74, 91, 101, 102, 115-131, and 133 have been cancelled.

IV. Status of Amendments

There were no amendments filed after the final office action dated as mailed July 31, 2007. Applicants chose to proceed directly with this appeal. All previous papers filed by Applicants have been entered.

V. Summary of Claimed Subject Matter

The present invention is a system and method for ensuring that information content data is presented in the same format to all requestors, clients or viewers. The information content data is capable of being presented in formats other than a predetermined format at different requestors or clients. Formatting data or data used to format the information content data is encrypted to prevent the formatting data from being corrupted or altered. The formatting data is encrypted and decrypted using at least one key or password to prevent the associated information content data from being presented in a format other than the predetermined format at each requestor or client to provide presentation integrity between the different requestors, clients or viewers. In another embodiment of the present invention, the system or method ensures that the proper version of multiple different versions of the content is presented to a particular audience or receiver. This is accomplished by encrypting the formatting data using a key corresponding to the version of the content for the particular audience or receiver.

Claims 1, 21, 34, 40, 48, 55, 62, 73, 90, 100, 108, 132, and 138 are independent claims and stand rejected in the present application. Claims 2-7 and 8-20 depend either directly or indirectly from independent claim 1; claims 22-33 depend directly or indirectly from independent claim 21; claims 35-39 depend directly or indirection from independent claim 34; claims 41-47 depend directly or indirectly from independent claim 40; claims 49-51 and 53-54 depend directly or indirectly from independent claim 48; claims 56-61 depend directly or indirectly from independent claim 55; claims 63-72 depend directly or indirectly from independent claim 62; claims 75-89 depend directly or indirectly from independent claim 73; claims 92-99 depend directly or indirectly from independent claim 90; claims 103-107 depend directly from independent claim 100; claims 109-114 depend directly from independent claim 108; claims 134-137 depend directly or indirectly from independent claim 132; and claims 139-141 depend

directly or indirectly from independent claim 138. All of these dependent claims stand rejected in the present application.

Independent claim 1 is a system claim. Claim 1 recites:

> "A system for presentation integrity, comprising an encrypter embodied in a data processing device to encrypt formatting data associated with information content data."

This feature of claim 1 is described in the specification in paragraphs [0020], [0030], [0037], and [0041]. This feature of claim 1 is also shown in Figure 1, reference numeral 102; Figure 3, reference numeral 302; Figure 5, reference numeral 502; and Figure 6, reference numeral 614.

Claim 1 also recites:

> "a formatter embodied in another data processing device to decrypt the encrypted formatting data and to format the information content data in a predetermined format based on the decrypted formatting data, wherein the information content data is capable of being presented in a format other than the predetermined format at different requesters or clients, and wherein the formatting data is encrypted and decrypted in response to at least one key or password to prevent the associated information content data from being presented in the format other than the predetermined format at each requester or client to provide presentation integrity between the different requesters or clients."

These features of claim 1 are described in the Specification in paragraphs [0023], [0032], [0033], and [0045]. These features of claim are also shown in the drawings in Figure 1, reference numeral 130; Figure 3, reference numeral 324; Figure 5, reference numeral 526; and Figure 6, reference numeral 628.

Dependent claim 3 is a system claim which depends directly from independent claim 1. Claim 3 recites:

> "wherein the formatter formats the information content data into one of a plurality of predetermined formats, each predetermined format corresponding to a different version of the information content data for presentation to different receivers or audiences, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information

> content data in response to applying the key associated with the selected predetermined format to the formatter, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver."

These features of claim 3 are described in the Specification in paragraph [0028], in Figure 2B blocks 220 and 222, and paragraphs [0034] and [0045].

Independent claim 21 is a system claim. Independent claim 21 recites a formatter with similar features to independent claim 1 and a device to present the information content data in the predetermined format. The device is described in the specification in paragraphs [0023], [0033], [0039] and [0045] and in the drawings in Figure 1, reference numeral 132; Figure 3, reference numeral 332; Figure 5, reference numeral 530; and Figure 6, reference numeral 630.

Dependent claim 23 is a system claim and depends directly from independent claim 21. Dependent claim 23 recites features similar to dependent claim 3.

Dependent claim 24 is a system claim and depends directly from dependent claim 23. Dependent claim 24 also includes features similar to dependent claim 3 previously discussed.

Independent claim 34 is a system claim which recites features similar to independent claim 1 and includes "a decrypter embodied in another data processing device to decrypt the formatting data." This feature is described in paragraph [0044] and in Figure 6, reference numeral 624.

Dependent claim 35 is a system claim and depends directly from independent claim 34. Claim 35 recites similar features to dependent claim 3 previously discussed.

Independent claim 40 is a system claim and recites a formatter with similar features to independent claim 1. Claim 40 also recites:

> "an encrypter operable on a server to encrypt information content data and formatting data associated with the information content data."

This feature of claim 40 is described in the Specification in paragraph [0030] and in Figure 3, reference numeral 302. Claim 40 also recites:

> "an information broker operable on the server to transmit the
> encrypted information content data and the encrypted formatting
> data to a client in response to an information request."

This feature of claim 40 is described in the Specification in paragraph [0031] and is shown in Figure 3 as reference numeral 316.

Independent claim 48 is a device claim. Claim 48 recites:

> "an encrypter to encrypt formatting data associated with
> information content data, wherein the formatting data is encrypted
> using a selected key or password to prevent the associated
> information content data from being presented in a format other
> than the predetermined format at each requester or client to provide
> presentation integrity between different requesters or clients."

This feature of independent claim 48 is described in the Specification in paragraph [0030] and is shown in Figure 3, reference numeral 302. Claim 48 also recites:

> "an information broker to transmit the encrypted formatting data
> and the associated information content data to each requestor or
> client in response to a request."

This feature of independent claim 48 is described in the Specification in paragraph [0031] and is shown in Figure 3, reference numeral 316.

Independent claim 55 is a device claim. Claim 55 recites a formatter including features similar to those of independent claim 1.

Dependent claim 56 is a device claim and depends directly from independent claim 55. Claim 56 recites features similar to dependent claim 3 as discussed above.

Claim 62 is an electronically-readable medium claim or computer product claim. Claim 62 recites:

> "information content data and formatting data applicable to the
> information content data to form the information content data in a
> predetermined format, wherein the information content data is
> capable of being presented in a format other than the
> predetermined format at different requesters or clients, and wherein
> the formatting data is encrypted and is decryptable by a data

> processing device in response to at least one key or password to
> prevent the information content data from being presented in the
> format other than the predetermined format at each requester or
> client to provide presentation integrity between the different
> requesters or clients."

These features of independent claim 62 are described in paragraph [0028] and in Figure 2B, block 220.

Dependent claim 65 is an electronically-readable medium or computer program product claim and depends directly from independent claim 62. Claim 65 recites features similar to claim 3 discussed above.

Independent claim 73 is a method claim. Claim 73 recites similar features to independent claim 1.

Independent claims 90 and 100 are method claims. Claims 90 and 100 recite features similar to independent claim 1.

Independent claim 108 is a method claim. Claim 108 recites:

> "decrypting encrypted formatting data associated with information
> content data."

This feature is described in the Specification in paragraph [0027] and in Figure 2B block 216. Claim 108 also recites:

> "formatting the associated information content data in one of a
> plurality of predetermined formats based on the decrypted
> formatting data, each predetermined format corresponding to a
> different version of the information content data for presentation to
> different receivers or audiences, wherein the information content
> data is distributable in one form or medium for all audiences or
> receivers and which version is presented is controlled by entering
> an appropriate key corresponding to the version for a particular
> audience or receiver."

This feature of claim 108 is described in the Specification in paragraph [0028] and in Figure 2B in block 220.

Independent claim 132 is a computer-readable medium claim. Claim 132 recites similar features to independent claim 100.

Independent claim 138 is a computer-readable medium claim. Claim 138 recites similar features to claim 108.

VI. Grounds of Rejection to be Reviewed on Appeal

1.   Whether claims 1-7, 9-14, 21-27, 31-36, 40-41, 45-49, 53-60, 62-73, 75-76, 78-85, 90, 92-94, 100, 103-110, 112-114, 132, and 134-141 are unpatentable under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Publication 2004/0225891 to Kang et al. (hereinafter Kang).

2.   Whether claim 15-20, 37-39, 50-51, 61, 86-89, and 95-99 are unpatentable under 35 U.S.C. § 103(a) as being unpatentable over Kang in view of U.S. Patent Publication No. 2003/0229529 to Mui et al. (hereinafter Mui).

3.   Whether claims 77 and 111 are unpatentable under 35 U.S.C. § 103(a) as being unpatentable over Kang in view of U.S. Patent Publication No: 2002/0099947 to Evans (hereinafter Evans).

4.   Whether claims 28-30 and 42-44 are unpatentable under 35 U.S.C. § 103(a) as being unpatentable over Kang in view of U.S. Patent 5,815,809 to Ward et al. (hereinafter Ward).

VII. Arguments

Rejection Under 35 U.S.C. § 102(e) as being anticipated by Kang

Claims 1, 2, 4-7, 9-14, 21-22, 26-27, 31-34, 40-41, 47-49, 53-55, 60, 62-64, 68-73, 75, 79-85, 90, 92-94, 100, 105-107, 132, 134, and 137

Turning initially to the rejection of independent claim 1 under 35 U.S.C. § 102(e) as being anticipated by Kang, claim 1 recites:

> "an encrypter embodied in a data processing device to encrypt formatting data associated with information content data..."

FIG. 19 steps S250 and S260 of Kang were cited in the Final Office Action dated as mailed 07/31/07 for rejecting this feature of independent claim 1. Kang in FIG. 19 in S250 teaches

generating header information and in S260 encrypting the header information. Applicant respectfully submits that S250 and S260 in FIG. 19 do not teach or suggest that the header is formatting data or includes formatting data and the Examiner is incorrectly reading this limitation into Kang. As further evidence that Kang does not teach or suggest formatting data in the header, Kang in paragraph [0106] recites:

> "[0106] The header information includes information necessary for encryption of the digital content such as size of the encrypted block, encryption period and encrypted frame unit, etc. The header information is also generated to include the hash value by applying the whole header to the hash algorithm, with which value the change of header information can be determined. The header information generated at the step of S250 is encrypted (S260) and then the information on the encrypted header and the size of the encrypted header is added to the header (S270), so that generated is the header added to the front end of the encrypted digital content transmitted to the user."

Additionally, Kang in paragraph [0099] recites:

> "[0090] FIG. 17 illustrates the details of an arrangement of an encrypted header that is suitable use in the header field shown by FIGS. 12 and 13. The encrypted header field may be arranged with a first field that indicates the basic process unit of the digital content of the information to be furnished to the user, a second field that indicates the number of encrypted bytes, a second field that states the encrypted frame unit, and a third, or hash value field, that establishes the state of the entire header. The basic process unit of the digital information and the number of the encrypted bytes of resulting from encryption of the digital information may be assigned by the information provider; however, the basic process unit and the number of encrypted bytes are likely to be set to basic values by a basic algorithm by reference to the processing speed of the terminal unit and a memory that stores data for the microprocessor based terminal unit. The hash value in the hash value field indicates the hash value of both the copyright support information field and the unencrypted header field; that is, the hash value for the fields arranged within the header field prior to the encrypted header field."

Applicant respectfully submits that Kang does not teach or suggest that the header information contains formatting data associated with the content data as required by claim 1. Additionally, claim 1 recites:

> "...wherein the information content data is capable of being presented in a format other than the predetermined format at different requesters or clients, and wherein the formatting data is encrypted and decrypted in response to at least one key or password to prevent the associated information content data from being presented in the format other than the predetermined format at each requester or client to provide presentation integrity between the different requesters or clients."

The Examiner cited paragraphs [0068], [0076] and [0091] of Kang for rejecting these features of independent claim 1. Applicant respectfully submits that none of these paragraphs teach or suggest the features of the embodiment of the present invention in claim 1 recited above. Paragraph [0068] of Kang recites:

> "[0068]   The interface 201 receives the key information that has been generated by service server 210 in dependence upon the user's identity characters. User authorization identifier 202 obtains the user's key after reading the header of the copyright protection protocol received from service server 210, and then determines whether the user is authorized to receive digital information by analyzing the user's authorization information with the user's key that has been generated. Temporary validation key decryptor 203 decrypts the temporary validation key by using the user's key provided by user authorization identifier 202. Digital content decryptor 204 decrypts the encrypted digital information received with the copyright protection protocol by using the temporary validation key decrypted by temporary validation key decryptor 203."

Paragraph [0068] of Kang is concerned with determining whether the user is authorized to receive digital information by analyzing the user's authorization information with the user's key that has been generated. This paragraph is also concerned with decrypting the encrypted digital information with the copyright protocol. This portion of Kang does not teach or suggest encrypting the formatting data to prevent the associated information content data from being presented in a format other than the predetermined format at each requestor or client to provide

presentation integrity between the different requestors or clients as provided by the embodiment of the present invention as recited in claim 1 above.

Kang in paragraph [0076] describes how user validation keys are generated. Beginning at line 15 of paragraph [0076], Kang recites:

> "The user's authorization information furnished by generator 215 is applied to header gcnerator 216, which adds the user authorization information to the header and then provides the header to protocol format generator 217. Protocol format generator 217 forms thc copyright protection protocol format by adding thc encrypted digital information to the header and then transmits the copyright protection protocol to thc user's terminal unit 200."

Again, Kang is only concerned with authorization and copyright protection protocol and does not teach or suggest encrypting the formatting data to prevent the associated information content data from being presented in a format other than the predetermined format at each requestor or client to provide presentation integrity as provided by the present invention.

Additionally, paragraph [0091] of Kang, referenced in rejecting claim 1, recites:

> "[0091]   FIG. 10 is an illustration of one protocol format as applied to the practice of the present invention. The format of one protocol for protecting the copyright of digital information to be transmitted by a service server, may be arranged with a header that includes information for encrypting the digital information and material that explains the digital information, and an encrypted digital information field. Referring additionally now to FIG. 5, to understand the structure of the header recall that the digital information requcsted by the user is encrypted partly by the user key and the temporary validation key so as to prevent replay of the digital information in the absence of the key information, such as when the encrypted digital information is obtained by another entity."

Again, paragraph [0091] of Kang is teaching prevention of unauthorized access to the digital information and protecting the copyright of the digital information. Paragraph [0091] of Kang also does not teach or suggest that the formatting data in encrypted and decrypted to prevent the associated information content data from being presented in the format other than the

predetermined format at each requested or client to provide presentation integrity between the different requesters or clients as provided by the embodiment of the present invention in independent claim 1.

For all of the reasons discussed above, Applicant respectfully submits that claim 1 includes elements that are not taught or suggested by Kang. Thus, claim 1 is patentably distinguishable over Kang. Reconsideration and withdrawal of the 35 U.S.C. § 102 rejection of claim 1 is respectfully requested.

Independent claims 21, 34, 40, 48, 55, 62, 73, 90, 100, and 132 recite similar features to independent claim 1. Additionally, the Examiner cited the same paragraphs of Kang in rejecting the features of these independent claims. These independent claims are also respectfully submitted to be patentably distinguishable over Kang for the same reasons as discussed with respect to independent claim 1. Reconsideration and withdrawal of the Section 102 rejection of these claims is respectfully solicited.

Claims 2, 4-7, and 9-14 depend either directly or indirectly from independent claim 1. Claims 22, 26-27, and 31-33 depend directly from independent claim 21. Claims 41 and 47 depend directly from independent claim 40. Claims 49, 53 and 54 depend directly from independent claim 48. Claim 60 depends directly or indirectly from independent claim 55. Claims 63-64 and 68-72 depend either directly or indirectly from independent claim 62. Claims 75 and 79-85 depend directly or indirectly from independent claim 73. Claims 92-94 depend directly from independent claim 90. Claims 105-107 depend directly from independent claim 100. Claims 134 and 137 depend directly from independent claim 132. Because of these dependencies, these dependent claims include all of the features of the referenced independent claim and any intermediate dependent claims. Accordingly, these dependent claims are respectfully submitted to be patentably distinguishable over Kang for the same reasons as discussed with respect to the independent claims. Reconsideration and withdrawal of the Section 102 rejection of these claims is, therefore, respectfully solicited.

Claim 3

Claim 3 recites:

> "...wherein the formatter formats the information content data into one of a plurality of predetermined formats, each predetermined format corresponding to a different version of the information content data for presentation to different receivers or audiences, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the formatter, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver."

The Examiner cited paragraph [0096] in rejecting claim 3. Kang in the pertinent parts of paragraph [0096] recites:

> "[0096]   FIG. 14 illustrates the format of an unencrypted header field suitable for the header fields of the alternatives shown by FIGS. 12 and 13. The unencrypted header field may be arranged with a copyright library version field, a digital conversion format field for indicating the type of the digital conversion format... The digital conversion format field shows which conversion technique was used to convert the digital content into the digital signal. Typical examples of the conversion method are MP3 and AAC."

Accordingly, Kang teaches that the digital conversion format field is an unencrypted header field. Thus, Kang teaches away from the present invention. Additionally, the digital conversion format field in Kang shows the type of digital conversion format, such as MP3 or AAC, and not which predetermined format corresponding to a different version of the content is formatted for presentation to a particular audience as provided by the embodiment of the present invention in claim 3. Kang does not teach or suggest that the information content data is distributable in one form or medium for all audiences and which version is presented is controlled by entering the appropriate key corresponding to the version for the particular audience. Accordingly, Applicant respectfully submits that Kang does not teach or suggest the features of claim 3. Additionally,

claim 3 depends directly from independent claim 1, and by virtue of that dependency, contains all of the features of independent claim 1. For all of these reasons, claim 3 is respectfully submitted to be patentably distinguishable over Kang, and reconsideration and withdrawal of the 35 U.S.C. § 102 rejection of claim 3 is respectfully requested.

Claims 23-25

Claims 23-25 recite similar features to claim 3. Additionally, claims 23-25 depend either directly or indirectly from independent claim 21. As a result of this dependency, claims 23-25 include all of the features of independent claim 21 and any intermediate claims. For all of these reasons, claims 23-25 are respectfully submitted to be patentably distinguishable over Kang for the same reasons as discussed with respect to claim 3 and independent claim 21. Reconsideration and withdrawal of the Section 102 rejection of claims 23-25 is respectfully solicited.

Claims 35-36 and 45-46

Claims 35-36 depend directly from independent claim 34 and claims 45-46 depend directly from independent claim 40. Because of these dependencies claim 35-36 include all of the features of claim 35 and claims 45-46 include all of the features of claim 40. Additionally, these claims recited features similar to claim 3 discussed above. For all of these reasons, claims 35-36 and 45-46 are submitted to be patentable over Kang for the same reasons as discussed with respect to independent claims 34 and 40 and claim 3. Reconsideration and withdrawal of the 35 U.S.C. §102 rejection of these claims is respectfully requested.

Claims 56-59

Claims 56-59 recite similar features to claim 3. Additionally, claims 56-59 depend either directly or indirectly from independent claim 55, and by virtue of that dependency include all of

the features of claim 55. Accordingly, claims 56-59 are respectfully submitted to be patentably distinct over Kang for the same reasons as discussed with respect to claims 3 and 55.

Claims 65-67, 76, 78, 103-104, and 135-136

Claims 65-67 depend directly from independent claim 62. Claims 76 and 78 depend directly from independent claim 73. Claims 103-104 depend directly from independent claim 100, and claims 135-136 depend either directly or indirectly from independent claim 132. As a result of these dependencies, each of these dependent claims includes all of the features of the referenced independent claim and any intermediate claims. Additionally, these claims recited features similar to claim 3 discussed above. For all of these reasons, claims 65-67, 76, 78, 103-104, and 135-136 are respectfully submitted to be patentable over Kang. Reconsideration and withdrawal of the Section 102 rejection of these claims is respectfully solicited.

Claims 108-114 and 138-141

Independent claims 108 and 138 recite features similar to claim 3. As discussed with respect to claim 3, Kang does not teach or suggest the features of formatting the information content and data in one of a plurality of predetermined formats based on the decrypted formatting data where each predetermined format corresponds to a different version of the information content data for presentation to different receivers or audiences. Kang also does not teach that the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver, as provided by the embodiment of the present invention as recited in independent claims 108 and 138. Accordingly, independent claims 108 and 138 are respectfully submitted to be patentably distinct over Kang, and reconsider and withdrawal of the 35 U.S.C. § 102 rejection of claims 108 and 138 is respectfully requested.

Claims 109-114 depend either directly or indirectly from independent claim 108. Claims 139-141 depend either directly or indirectly from independent claim 138. By virtue of these dependencies, each of these dependent claims includes all of the features of the reference

independent claim and any intermediate claims. Therefore, claims 109-114 and 139 and 141 are respectfully submitted to be patentably distinguishable over Kang for the same reasons as discussed with respect to independent claims 108 and 138. Reconsideration and withdrawal of the Section 102 rejection of claim 109-114 and 139-141 is respectfully requested.

Rejection Under 35 U.S.C. § 103(a) as being unpatentable over Kang in view of Mui

Claims 15-20, 37-39, 50-51, 61, 86-89, and 95-99

Claims 15-20 depend either directly of indirectly from independent claim 1; claims 37-39 depend either directly of indirectly from independent claim 34; claims 50-51 depend either directly of indirectly from independent claim 48; claim 61 depends directly from independent claim 55; claims 86-89 depend directly from independent claim 73; and claims 95-99 depend either directly of indirectly from independent claim 90. Because of these dependencies, these claims include all of the features of the referenced independent claims and any intervening claims. Mui was cited for teaching XSLT being used to produce HTML. Applicant respectfully submits that Mui adds nothing to the teachings of Kang so as to render independent claims 1, 34, 48, 55, 73 and 90 unpatentable. Therefore, these dependent claims are also respectfully submitted to be patentably distinguishable over Kang and Mui for the same reasons as discussed with respect to the independent claims. Reconsideration and withdrawal of the 35 U.S.C. § 103 rejection of these claims is respectfully requested.

Rejections under 35 U.S.C. § 103(a) as being unpatentable over Kang in view of Evans

Claims 77 and 111

Claim 77 depends indirectly from independent claim 73 and claim 111 depends directly from independent claim 108. Evans was cited for teaching the information content data comprising one of audio, visual, or combination audio/visual work. Applicant respectfully

submits that Evans adds nothing to the teachings of Kang so as to render independent claims 73 and 108 unpatentable. Therefore, claims 77 and 111 are respectfully submitted to be patentably distinguishable over Kang and Evans for the same reasons as discussed with respect to independent claims 73 and 108. Reconsideration and withdrawal of the Section 103 rejection of claims 73 and 111 is respectfully requested.

Rejection under 35 U.S.C. § 103(a) as being unpatentable over Kang in view of Ward

Claims 28-30 and 42-44

Claims 28-30 depend either directly or indirectly from independent claim 21 and claims 42-44 depend either directly or indirectly from independent claim 40. Because of these dependencies, claims 28-30 and 42-44 include all of the features of the referenced independent claim and any intermediate claims. Ward was disclosed for teaching a formatter in a vehicle and communication involving satellite and ground communications. Applicant respectfully submits that Ward adds nothing to the teachings of Kang so as to render independent claims 21 and 40 unpatentable. Therefore, dependent claims 28-30 and 40-44 are submitted to be patentably distinct over Kang and Ward, and reconsideration and withdrawal of the Section 103 rejection of these claims is respectfully solicited.
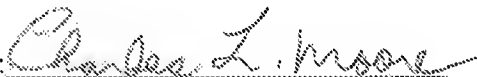
Conclusion

For the reasons stated above, Applicant respectfully submits that the rejections standing in this application are improper. The Examiner has failed to establish a *prima fascie* case of anticipation under 35 U.S.C. §102(e) with respect to claims 1-7, 9-14, 21-27, 31-36, 40-41, 45-49, 53-60, 62-73, 75-76, 78-85, 90, 92-94, 100, 103-110, 112-114, 132, and 134-141. With regard to claims 15-20, 28-30, 37-39, 42-44, 50-51, 61, 77, 86-89, 95-99, and 111, Applicant respectfully submits that the Examiner has failed to establish a *prima fascie* case of obviousness under 35 U.S.C. §103(a). Therefore, Applicant respectfully submits that claims 1-7, 9-51, 53-73, 75-90, 92-100, 103-114, 132, 134-141 are in condition for allowance. Reversal of the rejections of these claims are respectfully requested.

Respectfully submitted,

Peter L. Bergh
(Applicant)

Date: January 15, 2008   By: Charles L. Moore
Registration No. 33,742
Moore & Van Allen PLLC
P.O. Box 13706
Research Triangle Park, N.C. 27709
Telephone: (919) 286-8000
Facsimile: (919) 286-8199

VIII. Claims Appendix

1. (Previously Amended) A system for presentation integrity, comprising:

an encrypter embodied in a data processing device to encrypt formatting data associated with information content data; and

a formatter embodied in another data processing device to decrypt the encrypted formatting data and to format the information content data in a predetermined format based on the decrypted formatting data, wherein the information content data is capable of being presented in a format other than the predetermined format at different requesters or clients, and wherein the formatting data is encrypted and decrypted in response to at least one key or password to prevent the associated information content data from being presented in the format other than the predetermined format at each requester or client to provide presentation integrity between the different requesters or clients.

2. (Original) The system of claim 1, further comprising a plurality of formatters, each to decrypt the encrypted formatting data and to format the information content data in the predetermined format based on the decrypted formatting data.

3. (Previously Amended) The system of claim 1, wherein the formatter formats the information content data into one of a plurality of predetermined formats, each predetermined format corresponding to a different version of the information content data for presentation to different receivers or audiences, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the formatter, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.

4. (Original) The system of claim 1, wherein the formatter decrypts the formatting data to provide the predetermined format in response to each of a plurality of valid keys, each valid key being assigned to a different copy of the information content data.

5. (Original) The system of claim 1, further comprising an output device to present the information content data in the predetermined format.

6. (Original) The system of claim 5, wherein the output device comprises at least one of a display and a printer.

7. (Original) The system of claim 1, further comprising at least one of a computer and a media player to present the information content data in the predetermined format, wherein the formatter is embodied in the at least one of the computer or the media player.

8. Canceled

9. (Previously Amended) The system of claim 1, wherein the formatting data is encryptable and decryptable by a common key.

10. (Previously Amended) The system of claim 1, wherein the formatting data is encryptable and decryptable by different keys.

11. (Original) The system of claim 1, wherein the information content data is encryptable by the encrypter.

12. (Original) The system of claim 11, wherein the information content data and the formatting data are decryptable in response to a valid key.

13. (Original) The system of claim 11, wherein the information content data and the formatting data are each decryptable in response to different keys.

14. (Original) The system of claim 11, wherein the information content data and the formatting data are encryptable in response to different keys and are decryptable in response to keys that are each different from the keys used to respectively encrypt the information content data and the formatting data.

15. (Original) The system of claim 1, wherein the encrypter encrypts the formatting data into an encrypted style sheet language transformation (SLT).

16. (Original) The system of claim 15, wherein the SLT is an extensible style language transformation (XSLT).

17. (Original) The system of claim 15, wherein the formatter decrypts the encrypted SLT and transforms the information content data into a hypertext markup language (HTML) having the predetermined format in response to a valid password.

18. (Original) The system of claim 17, further comprising a browser to receive the information content data in HTML and to present the information content data in the predetermined format.

19. (Original) The system of claim 1, wherein the encrypter encrypts the information content data into an encrypted markup language (ML) and encrypts the formatting data into an encrypted style sheet transformation (SLT).

20. (Original) The system of claim 19, further comprising an information broker to transmit the information content data in the encrypted ML and the formatting data in the encrypted SLT to the formatter, wherein the formatter transforms the encrypted ML into an HTML format based on the SLT in response to the formatter receiving a valid password.

21. (Previously Amended) A system for presentation integrity, comprising:

     a formatter embodied in a data processing device to decrypt encrypted formatting data associated with information content data and to format the information content data into a

predetermined format based on the decrypted formatting data, wherein the information content data is capable of being presented in a format other than the predetermined format at different requesters or clients, and wherein the formatting data is decrypted in response to at least one key or password to prevent the associated information content data from being presented in the format other than the predetermined format at each information requester or client to provide presentation integrity between the different requesters or clients; and

a device to present the information content data in the predetermined format.

22. (Original) The system of claim 21, further comprising a plurality of formatters, each to decrypt the encrypted formatting data and to format the information content data in the predetermined format based on the decrypted formatting data.

23. (Original) The system of claim 21, wherein the formatter formats the information content data into one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the formatter.

24. (Previously Amended) The system of claim 23, wherein each predetermined format provides a different version of the information content data for presentation, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.

25. (Original) The system of claim 23, wherein the information content data is presentable in different versions of the information content for different audiences, wherein the information content comprises one of an audio, visual or combination audio-visual work, each version corresponding to one of the plurality of predetermined formats of the audio, visual or combination audio-visual work.

26. (Original) The system of claim 21, wherein the formatter decrypts the formatting data to provide the predetermined format in response to each of a plurality of valid keys, each valid key being assignable to a different copy of the information content data.

27. (Original) The system of claim 21, further comprising at least one of a computer and a media player to form the information content data in the predetermined format, wherein the formatter is embodied in the at least one of the computer or the media player.

28. (Original) The system of claim 21, wherein the formatter is adapted to be included in a vehicle.

29. (Original) The system of claim 28, wherein the vehicle comprises one of an aerospace vehicle, a watercraft and a terrestrial vehicle.

30. (Original) The system of claim 21, further comprising at least one of an aerospace communication channel and a terrestrial communication channel, wherein the formatter receives information content data and encrypted formatting data via at least one of the aerospace communication channel and the terrestrial communication channel.

31. (Original) The system of claim 21, wherein the formatter decrypts the information content data, if encrypted.

32. (Original) The system of claim 21, wherein the formatter decrypts the formatting data and the information content data, if encrypted, in response to a valid key.

33. (Original) The system of claim 21, wherein the formatter decrypts each of the formatting data and the information content data, if encrypted, in response to different keys.

34. (Previously Amended) A system for presentation integrity, comprising:

an encrypter embodied in a data processing device to encrypt formatting data associated with information content data;

a decrypter embodied in another data processing device to decrypt the formatting data; and

a formatter embodied in the other data processing device to format the information content data in a predetermined format based on the decrypted formatting data, wherein the information content data is capable of being presented in a format other than the predetermined format at different requesters or clients, and wherein the formatting data is encrypted and decrypted in response to at least one key or password to prevent the associated information content data from being presented in the format other than the predetermined format at each requester or client to provide presentation integrity between the different requesters or clients.

35. (Previously Amended) The system of claim 34, wherein the decrypter decrypts the formatting data to provide a selected one of a plurality of predetermined formats when the decrypted formatting data is applied to the information content data, each predetermined format corresponding to a different version of the information content data for presentation to different receivers or audiences, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide the selected one of the predetermined formats in response to applying the key associated with the selected predetermined format to the decrypter, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.

36. (Original) The system of claim 34, wherein the decrypter decrypts the formatting data to provide the predetermined format in response to each of a plurality of valid keys, each valid key being assignable to a different copy of the information content data.

37. (Original) The data processing device of claim 34, wherein the formatting data is encryptable into an encrypted SLT.

38. (Original) The system of claim 37, wherein the decrypter decrypts the encrypted SLT and transforms the information content data into a hypertext markup language (HTML) having the predetermined format in response to a valid password.

39. (Original) The system of claim 38, further comprising a browser to receive the transformed information content data in HTML and to form the information content data in the predetermined format.

40. (Previously Amended) A system for presentation integrity, comprising:

an encrypter operable on a server to encrypt information content data and formatting data associated with the information content data;

an information broker operable on the server to transmit the encrypted information content data and the encrypted formatting data to a client in response to an information request;

a formatter operable on a data processing device to decrypt the information content data and the formatting data and to format the decrypted information content data in a predetermined format based on the decrypted formatting data, wherein the information content data is capable of being presented in a format other than the predetermined format at different requesters or clients, and wherein the formatting data is encrypted and decrypted in response to at least one key or password to prevent the associated information content data from being presented in the format other than the predetermined format at each requester or client to provide presentation integrity between the different requesters or clients; and

a browser operable on the data processing device to present the information content data in the predetermined format.

41. (Original) The system of claim 40, further comprising a plurality of clients, each client including a formatter to decrypt the information content data and the formatting data and to format the decrypted information content data in the predetermined format on each client based on the decrypted formatting data .

42. (Original) The system of claim 41, wherein at least one client is adapted to be included in a vehicle.

43. (Original) The system of claim 42, wherein the vehicle is one of an aerospace vehicle, a watercraft and a terrestrial vehicle.

44. (Original) The system of claim 40, further comprising at least one of an aerospace communication channel and a terrestrial communication channel, wherein the formatter receives information content data and encrypted formatting data via at least one of the aerospace communication channel and the terrestrial communication channel.

45. (Previously Amended) The system of claim 40, wherein the formatter formats the information content data into one of a plurality of predetermined formats, each predetermined format corresponding to a different version of the information content data for presentation to different receivers or audiences, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the formatter, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.

46. (Original) The system of claim 40, wherein the formatter decrypts the formatting data to provide the predetermined format in response to each of a plurality of valid keys, each valid key being assignable to a different copy of the information content data.

47. (Original) The system of claim 40, wherein the information broker comprises one of a buffer and a storage device.

48. (Previously Amended) A device to process data, comprising:

an encrypter to encrypt formatting data associated with information content data, wherein the formatting data is encrypted using a selected key or password to prevent the associated information content data from being presented in a format other than the predetermined format at each requester or client to provide presentation integrity between different requesters or clients; and

an information broker to transmit the encrypted formatting data and the associated information content data to each requestor or client in response to a request.

49. (Original) The device of claim 48, wherein the encrypter encrypts the information content data.

50. (Original) The device of claim 49, wherein the information content data is encryptable into an encrypted markup language (ML) format.

51. (Original) The device of claim 50, wherein the formatting data is encryptable into a encrypted style sheet language transformation (SLT) format.

52. Canceled.

53. (Previously Amended) The device of claim 48, wherein the selected key is a different key from a key used to decrypt the encrypted formatting data.

54. (Original) The device of claim 48, wherein the information broker comprises one of a buffer and a storage device.

55. (Previously Amended) A device to process data, comprising:

a formatter to decrypt encrypted formatting data associated with information content data and to format the information content data into a predetermined format based on the decrypted formatting data, wherein the information content data is capable of being presented in a format other than the predetermined format at different requesters or clients, and wherein the

formatting data is decrypted using a selected key or password to prevent the associated information content data from being presented in the format other than the predetermined format at each requester or client to provide presentation integrity between different requesters or clients; and

an output device to present the information content data in the predetermined format.

56. (Previously Amended) The device of claim 55, wherein the formatter formats the information content data into one of a plurality of predetermined formats, each predetermined format corresponding to a different version of the information content data for presentation to different receivers or audiences, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the formatter, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.

57. (Original) The device of claim 56, wherein each predetermined format provides a different version of the information content data for presentation.

58. (Original) The device of claim 56, wherein the information content data is presentable in different versions of the information content for different audiences, wherein the information content comprises one of a motion picture, an audio, visual or combination audio-visual work, each version corresponding to one of the plurality of predetermined formats of the audio, visual or combination audio-visual work.

59. (Original) The device of claim 55, wherein the formatter decrypts the formatting data to provide the predetermined format in response to each of a plurality of valid keys, each valid key being assignable to a different copy of the information content data.

60. (Original) The device of claim 55, further comprising at least one of a computer and a media player to form the information content data in the predetermined format, wherein the formatter is embodied in the computer or the media player.

61. (Original) The device of claim 55, wherein the formatter transforms the information content data into a HTML format in response to a valid password, and wherein the device further comprises a browser to form the information content data in the predetermined format.

62. (Previously Amended) An electronically-readable medium having encoded thereon data structures, comprising:

information content data; and

formatting data applicable to the information content data to form the information content data in a predetermined format, wherein the information content data is capable of being presented in a format other than the predetermined format at different requesters or clients, and wherein the formatting data is encrypted and is decryptable by a data processing device in response to at least one key or password to prevent the information content data from being presented in the format other than the predetermined format at each requester or client to provide presentation integrity between the different requesters or clients.

63. (Original) The medium of claim 62, wherein the encrypted formatting data is decryptable by a selected key associated with a unique copy of the information content data.

64. (Original) The medium of claim 62, wherein the encrypted formatting data is decryptable by each of a plurality of keys, each key being associated with a different format to present the information content data based on decryption of the formatting data.

65. (Previously Amended) The medium of claim 62, wherein the information content is presentable in one of a plurality of predetermined formats, each predetermined format corresponding to a different version of the information content data for presentation to different

receivers or audiences, each predetermined format being associated with a different key, wherein the formatting data is decryptable to provide a selected one of the predetermined formats when applied to the information content data in response to applying the key associated with the selected predetermined format to the data processing device, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.

66. (Original) The medium of claim 62, wherein the information content data is presentable in different versions of the information content for different audiences, wherein the information content comprises one of an audio, visual or combination audio-visual work, each version corresponding to one of the plurality of predetermined formats of the audio, visual or combination audio-visual work.

67. (Original) The medium of claim 62, wherein the formatting data is decryptable to provide the predetermined format in response to each of a plurality of valid keys, each valid key being assignable to a different copy of the information content data.

68. (Original) The medium of claim 62, wherein the information content is encrypted.

69. (Original) The medium of claim 68, wherein the information content and the formatting data are decryptable in response to a valid key.

70. (Original) The medium of claim 68, wherein the information content and the formatting data are each decryptable in response to different keys.

71. (Original) The medium of claim 62, further comprising a marking to identify an authorized user of each copy of the information content data and encrypted formatting data.

72. (Original) The medium of claim 71, wherein the marking is formed by one of a public key signature, steganography or watermarking to identify the authorized user of each copy.

73. (Previously Amended) A method for presentation integrity, comprising:

decrypting encrypted formatting data associated with information content data;

and

formatting the associated information content data in a predetermined format based on the decrypted formatting data, wherein the information content data is capable of being presented in a format other than the predetermined format at different requesters or clients, and wherein the formatting data is encrypted and decrypted in response to at least one key or password to prevent the associated information content data from being presented in the format other than the predetermined format at each requester or client to provide presentation integrity between the different requesters or clients.

74. Canceled

75. (Original) The method of claim 73, further comprising sending the encrypted formatting data and the information content data to a plurality of clients, wherein the information content data is formatted in the predetermined format at each client.

76. (Original) The method of claim 73, wherein the information content data is presentable in one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to format the information content data in a selected one of the predetermined formats in response to a key associated with the selected predetermined format.

77. (Original) The method of claim 76, further comprising formatting the information content data into different versions for different audiences, wherein the information content data comprises one of an audio, visual, or combination audio-visual work, each version corresponding

to one of the plurality of predetermined formats of the audio, visual, or combination audio-visual work.

78. (Original) The method of claim 73, wherein the encrypted formatting data is decryptable to format an associated copy of the information content data in the predetermined format in response to a valid key assigned to the associated copy, wherein a different valid key is assigned to each copy of the information content data to only decrypt the formatting data associated with the assigned copy.

79. (Original) The method of claim 73, wherein the encrypted formatting data is decryptable in response to a valid key.

80. (Original) The method of claim 73, further comprising presenting the information content data in the predetermined format to each requestor providing a valid key.

81. (Original) The method of claim 80, wherein presenting the information content data comprises at least one of displaying or printing the information content data in the predetermined format.

82. (Original) The method of claim 73, further comprising decrypting the information content data, if encrypted.

83. (Original) The method of claim 73, wherein the encrypted formatting data and the information content data, if encrypted, are each decryptable in response to a valid key.

84. (Original) The method of claim 73, wherein the encrypted formatting data and the information content data, if encrypted, are each decryptable in response to a different key.

85. (Original) The method of claim 73, further comprising:
    updating the information content data; and

formatting the updated information content data in the predetermined format based on the decrypted formatting data.

86. (Original) The method of claim 73, further comprising encrypting the formatting data into an encrypted style sheet language transformation (SLT).

87. (Original) The method of claim 73, further comprising encrypting the information content data into an encrypted markup language (ML).

88. (Original) The method of claim 73, further comprising transmitting the information content data in an encrypted ML and the formatting data in an encrypted SLT to a requestor.

89. (Original) The method of claim 73, further comprising transmitting the information content data in the predetermined format in hypertext markup language (HTML) to a requestor.

90. (Previously Amended) A method for presentation integrity, comprising:
    accessing a chosen information page via a browser;
    decrypting encrypted formatting data associated with the chosen information page;
    formatting the chosen information page in a predetermined format based on the formatting data, wherein the chosen information page is capable of being presented in a format other than the predetermined format at different users including different types of browsers and browser settings;
    preventing the chosen information from being formatted other in the predetermined format at each user to provide presentation integrity between the different users; and
    presenting the chosen information page in the predetermined format.

91. Canceled

92. (Original) The method of claim 90, further comprising presenting the chosen information page in the predetermined format to each user in response to the user entering a valid password.

93. (Original)The method of claim 90, wherein the chosen information page is presentable in one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to format the chosen information page in a selected one of the predetermined formats in response to a key associated with the selected predetermined format.

94. (Original) The method of claim 90, wherein the encrypted formatting data is decryptable in response to a valid password.

95. (Original) The method of claim 90, further comprising:

presenting any parameter options for selection by a user; and

modifying the chosen information page in response to any parameter options selected by the user.

96. (Original) The method of claim 90, further comprising:

transforming the chosen information page from a markup language to HTML in the predetermined format based on the formatting data structure in SLT; and

transmitting the chosen information page in HTML to the browser.

97. (Original) The method of claim 96, further comprising transmitting the selected information page from a server to a client in HTML.

98. (Original) The method of claim 96, further comprising transmitting the selected information page from a server to a client in an encrypted ML.

99. (Original) The method of claim 96, further comprising transmitting the formatting data structure from a server to a client in an encrypted SLT.

100. (Previously Amended) A method for presentation integrity, comprising:

encrypting formatting data associated with information content data, wherein the information content data is capable of being presented in a format other than the predetermined format at different requesters or clients;

transmitting the information content data and the encrypted formatting data to at least one requestor; and

preventing the associated information content data from being presented in a format other than a predetermined format at each requester to provide presentation integrity between the different requesters.

101. Canceled

102. Canceled

103. (Previously Amended) The method of claim 100, wherein the information content data is presentable into one of a plurality of predetermined formats, each predetermined format corresponding to a different version of the information content data for presentation to different receivers or audiences, each predetermined format being associated with a different key, wherein the formatting data is decryptable to format the information content data in a selected one of the predetermined formats in response to a key associated with the selected predetermined format, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.

104. (Original) The method of claim 100, wherein the encrypted formatting data is decryptable to format an associated copy of the information content data in the predetermined format in response to a valid key assigned to the associated copy, wherein a different valid key is

assignable to each copy of the information content data to only decrypt the formatting data associated with the assigned copy.

105. (Original) The method of claim 100, further comprising encrypting the information content data.

106. (Original) The method of claim 100, wherein the encrypted formatting data and the information content data, if encrypted, are each decryptable in response to a valid key.

107. (Original) The method of claim 100, wherein the encrypted formatting data and the information content data, if encrypted, are each decryptable in response to a different key.

108. (Previously Amended) A method to control information content, comprising:

decrypting encrypted formatting data associated with information content data; and

formatting the associated information content data in one of a plurality of predetermined formats based on the decrypted formatting data, each predetermined format corresponding to a different version of the information content data for presentation to different receivers or audiences, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.

109. (Original) The method of claim 108, further comprising selecting one of the plurality of predetermined formats by decrypting the encrypted formatting data in response to a chosen one of a plurality of keys, each key corresponding to one of the plurality of predetermined formats.

110. (Original) The method of claim 109, further comprising formatting the information content data in each of the plurality of predetermined formats for a different intended audience.

111. (Original) The method of claim 108, wherein the information content data is one of an audio, visual or combination audio-visual work.

112. (Original) The method of claim 108, further comprising selecting one of a plurality of keys, each key corresponding to one of a plurality of predetermined formats to format the information content data, wherein the encrypted formatting data is decryptable in response to the selected one of the plurality of keys.

113. (Original) The method of claim 108, further comprising decrypting the encrypted formatting data and the information content, if encrypted, in response to a valid key.

114. (Original) The method of claim 108, further comprising decrypting the encrypted formatting data and the information content, if encrypted, in response to different keys.

115.-131. Canceled

132. (Previously Amended) A computer-readable medium encoded with computer-executable instructions for performing a method, comprising:

decrypting encrypted formatting data associated with information content data; and

formatting the associated information content data in a predetermined format based on the decrypted formatting data, wherein the information content data is capable of being presented in a format other than the predetermined format at different requesters or clients; and

preventing the associated information content data from being presented in the format other than the predetermined format at each requester or client to provide presentation integrity between the different requesters or clients.

133. Canceled

134. (Previously Amended) The computer-readable medium encoded with computer-executable instructions for performing the method of claim 132, further comprising sending the encrypted formatting data and the information content data to a plurality of clients, wherein the information content data is formatted in the predetermined format at each client.

135. (Previously Amended) The computer-readable medium encoded with computer-executable instructions for performing the method of claim 132, wherein the information content data is presentable in one of a plurality of predetermined formats, each predetermined format being associated with a different key, wherein the formatting data is decryptable to format the information content data in a selected one of the predetermined formats in response to a key associated with the selected predetermined format.

136. (Previously Amended) The computer-readable medium encoded with computer-executable instructions for performing the method of claim 135, further comprising formatting the information content data into different versions for different audiences, wherein the information content data comprises one of an audio, visual, or combination audio-visual work, each version corresponding to one of the plurality of predetermined formats of the audio, visual, or combination audio-visual work.

137. (Previously Amended) The computer-readable medium encoded with computer-executable instructions for performing the method of claim 132, wherein the encrypted formatting data is decryptable to format an associated copy of the information content data in the predetermined format in response to a valid key assigned to the associated copy, wherein a different valid key is assigned to each copy of the information content data to only decrypt the formatting data associated with the assigned copy.

138. (Previously Amended) A computer-readable medium encoded with computer-executable instructions for performing a method, comprising:

decrypting encrypted formatting data associated with information content data; and

formatting the associated information content data in one of a plurality of predetermined formats based on the decrypted formatting data, each predetermined format corresponding to a different version of the information content data for presentation to different receivers or audiences, wherein the information content data is distributable in one form or medium for all audiences or receivers and which version is presented is controlled by entering an appropriate key corresponding to the version for a particular audience or receiver.

139. (Previously Amended) The computer-readable medium encoded with computer-executable instructions for performing the method of claim 138, further comprising selecting one of the plurality of predetermined formats by decrypting the encrypted formatting data in response to a chosen one of a plurality of keys, each key corresponding to one of the plurality of predetermined formats.

140. (Previously Amended) The computer-readable medium encoded with computer-executable instructions for performing the method of claim 139, further comprising formatting the information content data in each of the plurality of predetermined formats for a different intended audience.

141. (Previously Amended) The computer-readable medium encoded with computer-executable instructions for performing the method of claim 139, further comprising selecting one of a plurality of keys, each key corresponding to one of a plurality of predetermined formats to format the information content data, wherein the encrypted formatting data is decryptable in response to the selected one of the plurality of keys.

IX. Evidence Appendix

None.

X. Related Proceedings Appendix

None